AGENCY OF HUMAN SERVICES

AHS Information Access and Information Flow Standard

Jack Green

10/3/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Information Access and Information Flow (AC-4, AC-14, AC-14(1), AC-17, AC-17(1), AC-17(3), AC-20) Controls.

Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
10/3/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:
The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Information Access and Information Flow (AC-4, AC-14, AC-14(1), AC-17, AC-17(1), AC-17(3), AC-20) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE
The scope of this standard includes the VHC and its constituent systems only.

STANDARD

Web Browser Access

1. The VHC Website is accessible by going to the URL http://healthconnect.vermont.gov/
    - Permitted without identification and authentication
2. The VHC Customer Portal is accessible by going to the URL https://portal.healthconnect.vermont.gov/
    - Access to information beyond this point requires identification and authorization
3. The VHC State Portal is accessible by going to the URL https://
    - Access to information beyond this point requires identification and authorization

Comment [RB1]: What is the state portal URL?

VPN/Remote Access

1. VHC WAN systems are VPN or remote connection. The user must first log into the VHC VPN using login credentials. Once the user is on the VPN, they then can log into the VHC WAN system required.
2. All web based systems can be logged into via VPN by connecting first to the VPN client then launching the browser window and accessing the website URLs.

Administrative Access

1. Instructions for Administrative Access are provided in a separate document available to authorized users. Authorized users may request the document from the ISO.

Comment [RB2]: Who will be the holder of this document?

Internal/external Connection use and monitoring

1. All connections either internally or externally will be monitored at the VHC by the Security and Privacy Manager to ensure compliance.
2. The system owner must ensure that all connections (internal or external) are authorized and adhere to the Access Control Policy (AC-4) for Information Security. This coordination can be done with the Security and Privacy Manager to ensure compliance.

Information flow control

1. The Security and Privacy Manager will then employ enforcement mechanisms to control the flow of information between designated sources and destinations such as networks or other devices either internally or externally.
    - An Intrusion Prevention System (IPS) is used to log and prevent malicious attacks on the network and to block IP addresses of specific countries in order to minimize the location where these attacks can come from.

Determining appropriate information flow

1. All Information System Owners are to ensure proper documentation and authorization of all connections between external networks and the internal network.
2. Regulation of where information is allowed to go is enforced by the information system in accordance with the Access Control Policy for Information Security.
    - All export controlled information will not be permitted to be transported free and clear to the internet
    - All web requests passed to the internet are required to come from the internal web proxy.
    - All remote access to FTI data must be through an approved encrypted modem or VPN for every workstation, and a Smart Card for every user.
        i. Smart Cards must have identification, authentication, and encryption features.
        ii. Two-factor authentication is required whenever FTI data is being accessed from an alternative work location or if accessing FTI data via the VHC state web portal.
        iii. FTI data may not be accessed from the VHC customer portal.
    - Use of external information systems (workstations, tablets…) not explicitly authorized in writing by the system owner are prohibited.

- Use of authorized external information systems adhere to strict terms and conditions as established by the AC-20 access control.

Procedure for information review

1. VHC Connect administration will identify users who are permitted to publish public information. Only those users have the rights granted to share public information on any information system. Those identified users will attend training on public information sharing.

Authorization of information to be shared

1. The proposed content to be shared must go through a review to ensure non-public information is not shared. The review will be performed by the business owner and/or key stakeholders.

Publishing public information

1. Any public information shared after being approved will then be posted and annual reviews will take place to ensure the information does not contain any non-public information.
2. In the event non-public information is discovered, the content must be removed by the system administrator immediately.

IMPORTANT INFORMATION
These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec